(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 April 2004 (29.04.2004)

PCT

(10) International Publication Number
WO 2004/036892 A2

(51) International Patent Classification[7]: H04N

(21) International Application Number:
PCT/US2003/027775

(22) International Filing Date:
8 September 2003 (08.09.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/409,675	9 September 2002 (09.09.2002)	US
10/273,903	18 October 2002 (18.10.2002)	US
10/274,084	18 October 2002 (18.10.2002)	US
10/274,019	18 October 2002 (18.10.2002)	US
10/273,905	18 October 2002 (18.10.2002)	US

(71) Applicant: SONY ELECTRONICS INC. [US/US]; 1 Sony Drive, Park Ridge, NJ 07656 (US).

(72) Inventor: CANDELORE, Brant, L.: 10124 Quail Glen Way, Escondido, CA 92029-6502 (US).

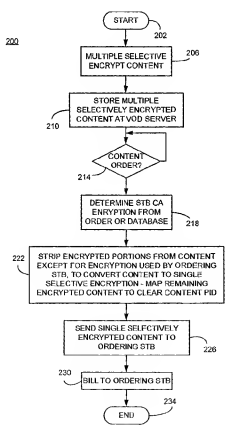
(74) Agents: KANANEN, Ronald, P. et al.; RADER FISHMAN & GRAUER PLLC, 1233 20th Street, NW, Suite 501, Washington, DC 20036 (US).

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO,

[Continued on next page]

(54) Title: SELECTIVE ENCRYPTION FOR VIDEO ON DEMAND



(57) Abstract: A video on demand (VOD) method, consistent with the invention involves storing multipleselective encrypted VOD content on a VOD server; receiving an order for the VOD contentspecifying delivery to a target decoder; determining what CA encryption system is associatedwith the order; stripping all encrypted segments from the multiple selectively encryptedcontentthat are not associated with the order to produce single selectively encrypted VOD content tothe target decoder. The multiple selectively encrypted VOD content can be created by examining unencrypted data representing digital content to identify segments of content for encryption; encrypting the identified segments fo content using a first encryption method associated with a first conditional access system to produce second encrypted segments; and replacing the identified segments of content with he first encrypted content and the second encrypted content in the digital content, to produce the multipe selectively encrypted VOD content.

WO 2004/036892 A2

SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SELECTIVE ENCRYPTION FOR VIDEO ON DEMAND

CROSS REFERENCE TO RELATED DOCUMENTS

This application is a continuation-in-part of U.S. patent applications serial number 10/273,905, filed October 18, 2002 to Candelore et al., entitled "Video Slice and Active Region Based Dual Partial Encryption", serial number 10/273,903, filed October 18, 2002 to Candelore et al., entitled "Star Pattern Partial Encryption", serial number 10/274,084, filed October 18, 2002 to Candelore et al., entitled "Slice Mask and Moat Pattern Partial Encryption", and serial number 10/274,019, filed October 18, 2002 to Candelore et al., entitled "Video Scene Change Detection", which are hereby incorporated by reference.

This application is also related to and claims priority benefit of U.S. Provisional patent application serial number 60/409,675, filed September 9, 2002, entitled "Generic PID Remapping for Content Replacement", to Candelore and U.S. Provisional Application serial number 60/351,771, filed January 24, 2002, entitled " Method for Allowing Multiple CA Providers to Interoperate in a VOD Delivery System and Content Delivered on Package Media" to Candelore. These applications are also hereby incorporated by reference herein.

COPYRIGHT NOTICE

A portion of the disclosure of this patent document contains material which is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction of the patent document or the patent disclosure, as it appears in the Patent and Trademark Office patent file or records, but otherwise reserves all copyright rights whatsoever.

FIELD OF THE INVENTION

This invention relates generally to the field of video on demand (VOD). More particularly, this invention relates to a multiple encryption method and apparatus particularly useful for multiple encrypting digitized video on demand programming.

BACKGROUND OF THE INVENTION

Video On Demand (VOD) is becoming a service which cable operators now consider to be a mandatory service as much as subscription and impulse pay-per-view (IPPV). But, VOD is different from broadcast services in that content is statically stored on VOD servers (often at the cable hubs), and is delivered to a specific subscriber upon receipt of a specific request by that subscriber.

VOD servers are often located at cable hub facilities. Hubs are located out in the local neighborhoods and serve a subset of perhaps about 80,000 subscribers. By locating the VOD system at the hub level, use of bandwidth is more efficient since customers in different hubs can use the same spectrum. As a point of contrast, subscription and IPPV content is generally scrambled at a Master Headend and delivered to the hubs for distribution.

There are currently two major VOD service providers in the cable industry. In one, content is stored pre-encrypted on hard drives in the VOD server. The keys used to encrypt the content do not change from month-to-month, however,

the entitlement control messages (ECMs) used to derive those keys to enable the conditional access (CA) system are updated every month. In the second VOD system, content is stored in-the-clear on hard drives in the VOD server. The content is encrypted real-time with slow changing keys (lasting 20 minutes or more). For other systems, the VOD content is sent in-the-clear to subscribers. Storage has been typically in-the-clear or encrypted using a simple "storage key".

The frequency and program identifiers (PIDs) used for a VOD session are privately signaled through encrypted transactions, so that someone trying to eavesdrop on the VOD communication cannot receive the tuning information for the program even if the content is sent in-the-clear. In some systems, the content is scrambled as an IPPV program. The program is therefore "purchased" as in a broadcast IPPV program. If an eavesdropper could locate the VOD channel, he or she would still need to pay for the movie as the legitimate customer.

In addition to the security provided by encryption, encryption of PIDs and frequencies and other measures, VOD security also relies on the fact that both the content and viewing times are under control of a legitimate purchasing party. That party can pause the program for a half an hour or all day. The content can be "rewound" or started over from scratch. These factors all contribute to providing protection against pirating of the content.

For all of the differences between VOD programming and conventional programming for cable and satellite programming, there remains a significant problem when a cable or satellite operator wishes to utilize decoder equipment (e.g., television set top boxes (STBs)) from multiple vendors. As with conventional cable television, each vendor generally uses its own conditional access (CA) encryption system. If a multiple service operator (MSO) chooses to utilize mulitple STBs in a system, it must somehow accommodate multiple CA systems. This problem has been discussed extensively in the above-referenced patent applications. Since VOD content storage is limited, duplicating content so

that it may be available to both legacy and non-legacy CAs may not be a practical (because of a lack of rack space), or economical (storage costs money).

BRIEF DESCRIPTION OF THE DRAWINGS

The features of the invention believed to be novel are set forth with particularity in the appended claims. The invention itself however, both as to organization and method of operation, together with objects and advantages thereof, may be best understood by reference to the following detailed description of the invention, which describes certain exemplary embodiments of the invention, taken in conjunction with the accompanying drawings in which:

FIGURE 1 is a block diagram of an exemplary video on demand cable television system consistent with certain embodiments of the present invention.

FIGURE 2 is a flow chart depicting operation of an exemplary embodiment consistent with certain embodiments of the present invention.

FIGURE 3 illustrates conversion from clear content to dual selectively encrypted content to single selectively encrypted content in a manner consistent with certain embodiments of the present invention.

FIGURE 4 is a block diagram of an exemplary video on demand server consistent with certain embodiments of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

While this invention is susceptible of embodiment in many different forms, there is shown in the drawings and will herein be described in detail specific embodiments, with the understanding that the present disclosure is to be considered as an example of the principles of the invention and not intended to limit the invention to the specific embodiments shown and described. In the description below, like reference numerals are used to describe the same, similar or corresponding parts in the several views of the drawings.

The terms "scramble" and "encrypt" and variations thereof are used synonymously herein. The term "video" may be used herein to embrace not only true visual information, but also in the conversational sense (e.g., "video tape recorder") to embrace not only video signals but associated audio and data. The present document generally uses the example of a "dual selective encryption" embodiment, but those skilled in the art will recognize that the present invention can be utilized to realize multiple partial encryption without departing from the invention. The terms "partial encryption" and "selective encryption" are used synonymously herein. Also, the terms "program" and "television program" and similar terms can be interpreted in the normal conversational sense, as well as a meaning wherein the term means any segment of A/V content that can be displayed on a television set or similar monitor device. The term "legacy" as used herein refers to existing technology used for existing cable and satellite systems. The exemplary embodiments disclosed herein are decoded by a television Set-Top Box (STB), but it is contemplated that such technology will soon be incorporated within television receivers of all types whether housed in a separate enclosure alone or in conjunction with recording and/or playback equipment or Conditional Access (CA) decryption module or within a television set itself. The present document generally uses the example of a "dual partial encryption" embodiment, but those skilled in the art will recognize that the present invention can be utilized to realize multiple partial encryption without departing from the invention.

The above-referenced commonly owned patent applications describe inventions relating to various aspects of methods generally referred to herein as partial encryption or selective encryption. More particularly, systems are described wherein selected portions of a particular selection of digital content are encrypted using two (or more) encryption techniques while other portions of the content are left unencrypted. By properly selecting the portions to be encrypted, the content can effectively be encrypted for use under multiple

decryption systems without the necessity of encryption of the entire selection of content. In some embodiments, only a few percent of data overhead is needed to effectively encrypt the content using multiple encryption systems. This results in a cable or satellite system being able to utilize Set-top boxes or other implementations of conditional access (CA) receivers from multiple manufacturers in a single system - thus freeing the cable or satellite company to competitively shop for providers of Set-top boxes.

The present invention applies similar selective encryption techniques to the problem of multiple VOD encryption systems. The partial encryption processes described in the above patent applications utilize any suitable encryption method. However, these encryption techniques are selectively applied to the data stream, rather than encrypting the entire data stream, using techniques described in the above-referenced patent applications. In general, but without the intent to be limiting, the selective encryption process utilizes intelligent selection of information to encrypt so that the entire program does not have to undergo dual encryption. By appropriate selection of data to encrypt, the program material can be effectively scrambled and hidden from those who desire to hack into the system and illegally recover commercial content without paying. MPEG (or similar format) data that are used to represent the audio and video data does so using a high degree of reliance on the redundancy of information from frame to frame. Certain data can be transmitted as "anchor" data representing chrominance and luminance data. That data is then often simply moved about the screen to generate subsequent frames by sending motion vectors that describe the movement of the block. Changes in the chrominance and luminance data are also encoded as changes rather than a recoding of absolute anchor data. Thus, encryption of this anchor data, for example, or other key data can effectively render the video un-viewable.

In accordance with certain embodiments consistent with the present invention, the selected video data to be encrypted may be any individual one or

combination of the following (described in greater detail in the above applications): video slice headers appearing in an active region of a video frame, data representing an active region of a video frame, data in a star pattern within the video frame, data representing scene changes, I Frame packets, packets containing motion vectors in a first P frame following an I Frame, packets having an intra_slice_flag indicator set, packets having an intra_slice indicator set, packets containing an intra_coded macroblock, data for a slice containing an intra_coded macroblock, data from a first macroblock following the video slice header,packets containing video slice headers, anchor data, and P Frame data for progressively refreshed video data, data arranged in vertical and or horizontal moat patterns on the video frame, and any other selected data that renders the video and/or audio difficult to utilize. Several such techniques as well as others are disclosed in the above-referenced patent applications, any of which (or other techniques) can be utilized with the present invention to encrypt only a portion of the content.

Referring now to **FIGURE 1**, a VOD content delivery system 100 consistent with certain embodiments of the present invention is illustrated. In this system, a cable television muliple services operator (MSO) operates a cable head end 104 to provide content to subscribers. VOD content is statically stored on VOD servers such as servers 108 and 112 depicted as located at cable hubs 116 and 120 respectively. The VOD content is delivered to a specific subscriber's STB such as STB 124, 128, 132 or 136 upon receipt of a specific request by that subscriber.

In accordance with certain embodiments consistent with the present invention, content stored in the VOD servers is delivered to the ordering STB which has an individual identification code that can be addressed by the cable head end and VOD server. Because VOD is interactive, the cable system can learn not only the address of the ordering STB, but also what type of STB the

ordering STB is (e.g., a legacy or non-legacy set-top box), and what CA system the STB uses.

Using selective encryption for subscription and IPPV broadcast services as described in the above-referenced patent applications, cable operators can manage content in real-time - received and decrypted off HITS satellites, and then selectively re-encrypted for the legacy and non-legacy conditional access (CA) providers operating in the cable plant. Such selective encryption entails duplicating and encrypting certain important or critical segments of the content independently with each CA while sending the remainder of the content in the clear. The clear content can be received by both legacy and non-legacy set-top boxes, affording a huge savings in bandwidth from the "full dual carriage" approach, while the encrypted content is decrypted by the respective set-top boxes with the particular CA.

In VOD systems, since the content is directed to a specific target STB (the ordering STB), the efficiency of both transmission and storage of the content can be enhanced using multiple and single selective encryption in accordance with embodiments consistent with the present invention. **FIGURE 2** depicts a process 200 consistent with an embodiment of the present invention starting at 202 in which the VOD content is stored as a multiple (e.g., dual) selectively encrypted content and then transmitted as single selectively encrypted content. At 206, the content is selectively multiply encrypted. This is carried out by selecting appropriate segments of content to be encrypted that are important or critical to the decoding of the content, duplicating those selected segments content and encrypting each copy using a different encryption method (one for each CA system in use). The resulting multiple selectively encrypted content is then stored on the VOD server(s) or at a data repository in the cable head end. Of course, those skilled in the art will understand that any time critical PCR information should be fixed along with the Continuity Counter information in the duplicated packets.

When VOD content is ordered by a subscriber at 214, the cable system (e.g., using registration information stored at the cable head end for each STB) determines what type of STB is associated with the order and thus what type of CA encryption system is being used by the ordering STB at 218. Once this is determined, there is no need to transmit the multiple selectively encrypted content to the subscriber (unless the order somehow is to be associated with multiple STBs of different types as in a household having two different STBs, both of which are to be entitled to decode the content). Thus, the encrypted portions of the content that are encrypted under a CA encryption not used by the ordering STB are stripped out at 222 to convert the multiple selectively encrypted VOD content into single selectively encrypted VOD content. The remaining encrypted content is then associated with the program identifier used by the clear unencrypted content to produce the single selectively encrypted VOD content. This single selectively encrypted VOD content is then provided to the ordering STB at 226. As a result of the order of the VOD content, a bill is ultimately sent to the subscriber at 230 for the VOD content and the process ends at 234.

Thus, in accordance with certain embodiments consistent with the present invention, a video on demand (VOD) method, involves storing multiple selective encrypted VOD content on a VOD server; receiving an order for the VOD content specifying delivery to a target decoder; determining what CA encryption system is associated with the order; stripping all encrypted segments from the multiple selectively encrypted content that are not associated with the order to produce single selectively encrypted VOD content; and sending the single selectively encrypted VOD content to the target decoder. The multiple selectively encrypted VOD content can be created by examining unencrypted data representing digital content to identify segments of content for encryption; encrypting the identified segments of content using a first encryption method associated with a first conditional access system to produce first encrypted segments; encrypting the identified segments of content using a second encryption method associated with

a second conditional access system to produce second encrypted segments; and replacing the identified segments of content with the first encrypted content and the second encrypted content in the digital content, to produce the multiple selectively encrypted VOD content.

The data streams or files representing the VOD content associated with this process are depicted in **FIGURE 3**. The clear content is represented by packets or other segments of data containing a "C" while encrypted segments encrypted under CA encryption system A is represented by the designations "CA-A". Encrypted segments encrypted under CA encryption system B is represented by designations "CA-B". The initial file is either unencrypted or decrypted and its initial 16 segments is shown as 310. In order to produce the multiply selectively encrypted file, in this case dual selectively encrypted, segments 7 and 14 are selected for encryption. These segments may correspond to important or critical data needed for decoding or may be selected according to any desired selection criteria. These segments are duplicated, encrypted under CA-A and CA-B and reinserted into the file or data stream as shown to produce the dual selectively encrypted file. This file 320 can then be stored for later retrieval, when a customer places an order for this VOD content, on one or more of the VOD servers at the cable hubs or at the cable head end. Once an order is placed, and the order is associated with a particular type of STB (the target STB or ordering STB) and thus a particular type of CA encryption, the dual selectively encrypted content is converted to single encrypted content for transmission to the ordering STB. This is done by stripping out the unneeded portions that are encrypted under any unused CA systems to produce a data stream such as that depicted in 330. In this case, CA-A encrypted segments are stripped out and CA-B encrypted segments remain.

Thus, by use of this technique the storage requirements of the VOD file servers are minimized by not requiring full multiple copies of encrypted content to be stored thereon. Still, the content is stored in a secure manner with low

overhead needed to accommodate the multiple encryption schemes. The content, when sent to the ordering STB is further optimized to eliminate the small amount of overhead used for the second CA encryption scheme to further enhance the efficiency of the utilization of the bandwidth for transmission of the VOD content to the ordering STB. Since the VOD system knows which set-top box, legacy or non-legacy, it is sending content to, the content does not need to be sent with packet duplication. This can preserve bandwidth on the cable plant. While the elimination of the un-needed packet is not strictly required, it provides the advantage of minimizing bandwidth and can eliminate the need for a "shadow" or secondary PID to be called out in the Program Map Table (PMT) as described in the above-referenced patent applications, since the encrypted packet can be mapped to the primary PID associated with the unencrypted content.

The process 200 of **FIGURE 2** can be carried out on any suitable programmed general purpose processor operating as a VOD server/encoder such as that depicted as computer 400 of **FIGURE 4**. Computer 400 has one or more central processor units (CPU) 410 with one or more associated buses 414 used to connect the central processor unit 410 to Random Access Memory 418 and Non-Volatile Memory 422 in a known manner. Output devices 426, such as a display and printer, are provided in order to display and/or print output for the use of the MSO as well as to provide a user interface such as a Graphical User Interface (GUI). Similarly, input devices such as keyboard, mouse and removable media readers 430 may be provided for the input of information by the operator. Computer 400 also incorporates internal and/or external attached disc or other mass storage 434 (e.g., disc and/or optical storage) for storing large amounts of information including, but not limited to, the operating system, multiple CA encryption methods (if encryption is carried out by the VOD server), as well as the VOD content (which is most likely stored on massive attached storage). The Computer system 400 also has an interface 438 for connection to

the cable system to service customer requests for content, and may also have interface 444 that interfaces to multiple encryption devices if the encryption is carried out by separate hardware. While depicted as a single computer, the digital content provider may utilize multiple linked computers to carry out the functions described herein.

In one embodiment of an electronic storage medium storing selectively encrypted video on demand (VOD) programming consistent with embodiments of the invention, stores a file representing multiple selective encrypted VOD content having: segments of unencrypted VOD content; first encrypted segments of VOD content encrypted using a first encryption method associated with a first conditional access system; second encrypted segments of VOD content encrypted using a second encryption method associated with a second conditional access system;

the first and second encrypted segments of VOD content representing the same segment of VOD content when not encrypted. A first segment of code, when executed operates to remove one of the first and second encrypted segments of VOD content from the multiple selective encrypted VOD content to produce single selectively encrypted content for transmission to a target decoder. The first segment of code operates to remove one of the first and second encrypted segments of VOD content upon receipt of an order for the VOD content specifying delivery to a target decoder, and upon determining which CA encryption system is associated with the order. The second segment of code sends the single selectively encrypted VOD content to the target decoder. A third segment of code associates a program identifier with the single selectively encrypted VOD content, wherein the same PIDs are used for encrypted and unencrypted segments of content.

Those skilled in the art will recognize that the present invention has been described in terms of exemplary embodiments based upon use of a programmed processor (e.g., computer 400). However, the invention should not be so limited,

since the present invention could be implemented using hardware component equivalents such as special purpose hardware and/or dedicated processors which are equivalents to the invention as described and claimed. Similarly, general purpose computers, microprocessor based computers, micro-controllers, optical computers, analog computers, dedicated processors and/or dedicated hard wired logic may be used to construct alternative equivalent embodiments of the present invention. Moreover, although the present invention has been described in terms of a general purpose personal computer providing a playback mechanism, the playback can be carried on a dedicated machine without departing from the present invention.

Those skilled in the art will appreciate that the program steps and associated data used to implement the embodiments described above can be implemented using disc storage as well as other forms of storage such as for example Read Only Memory (ROM) devices, Random Access Memory (RAM) devices; optical storage elements, magnetic storage elements, magneto-optical storage elements, flash memory, core memory and/or other equivalent storage technologies without departing from the present invention. Such alternative storage devices should be considered equivalents.

The present invention, as described in embodiments herein, is implemented using a programmed processor executing programming instructions that are broadly described above form that can be stored on any suitable electronic storage medium or transmitted over any suitable electronic communication medium or otherwise be present in any computer readable or propagation medium. However, those skilled in the art will appreciate that the processes described above can be implemented in any number of variations and in many suitable programming languages without departing from the present invention. For example, the order of certain operations carried out can often be varied, additional operations can be added or operations can be deleted without departing from the invention. Error trapping can be added and/or enhanced and

variations can be made in user interface and information presentation without departing from the present invention. Such variations are contemplated and considered equivalent.

Software code and/or data embodying certain aspects of the present invention may be present in any computer readable medium, transmission medium, storage medium or propagation medium including, but not limited to, electronic storage devices such as those described above, as well as carrier waves, electronic signals, data structures (e.g., trees, linked lists, tables, packets, frames, etc.) optical signals, propagated signals, broadcast signals, transmission media (e.g., circuit connection, cable, twisted pair, fiber optic cables, waveguides, antennas, etc.) and other media that stores, carries or passes the code and/or data. Such media may either store the software code and/or data or serve to transport the code and/or data from one location to another. In the present exemplary embodiments, MPEG compliant packets, slices, tables and other data structures are used, but this should not be considered limiting since other data structures can similarly be used without departing from the present invention.

While the invention has been described in conjunction with specific embodiments, it is evident that many alternatives, modifications, permutations and variations will become apparent to those skilled in the art in light of the foregoing description. Accordingly, it is intended that the present invention embrace all such alternatives, modifications and variations as fall within the scope of the appended claims.

What is claimed is:

1. A video on demand (VOD) method, comprising:

storing multiple selective encrypted VOD content on a VOD server;

receiving an order for the VOD content specifying delivery to a target decoder;

determining what CA encryption system is associated with the order;

stripping all encrypted segments from the multiple selectively encrypted content that are not associated with the order to produce single selectively encrypted VOD content; and

sending the single selectively encrypted VOD content to the target decoder.

2. The method according to claim 1, further comprising:

examining unencrypted data representing digital content to identify segments of content for encryption;

encrypting the identified segments of content using a first encryption method associated with a first conditional access system to produce first encrypted segments;

encrypting the identified segments of content using a second encryption method associated with a second conditional access system to produce second encrypted segments; and

replacing the identified segments of content with the first encrypted content and the second encrypted content in the digital content, to produce the multiple selectively encrypted VOD content.

3. The method according to claim 1, further comprising associating a program identifier with the single selectively encrypted VOD content, wherein the same PIDs are used for encrypted and unencrypted segments of content.

4. The method according to claim 1, wherein the decoder comprises a television Set-top box.

5. The method according to claim 1, wherein the VOD server resides at a cable hub.

6. A computer readable medium storing instructions which, when executed on a programmed processor, carry out the VOD method according to claim 1.

7. An electronic transmission medium carrying single selectively encrypted VOD content created by the method according to claim 1.

8. A video on demand (VOD) method, comprising:

examining unencrypted data representing digital content to identify segments of content for encryption;

encrypting the identified segments of content using a first encryption method associated with a first conditional access system to produce first encrypted segments;

encrypting the identified segments of content using a second encryption method associated with a second conditional access system to produce second encrypted segments;

replacing the identified segments of content with the first encrypted content and the second encrypted content in the digital content, to produce the multiple selectively encrypted VOD content;

storing the multiple selective encrypted VOD content on a VOD server residing at a cable hub;

receiving an order for the VOD content specifying delivery to a target decoder;

determining what CA encryption system is associated with the order;

stripping all encrypted segments from the multiple selectively encrypted content that are not associated with the order to produce single selectively encrypted VOD content;

associating a program identifier with the single selectively encrypted VOD content, wherein the same PIDs are used for encrypted and unencrypted segments of content; and

sending the single selectively encrypted VOD content to the target decoder.

9. A video on demand (VOD) encoder, comprising:

a programmed processor that examines unencrypted data representing digital content to identify segments of content for encryption;

a first encrypter that encrypts the identified segments of content using a first encryption method associated with a first conditional access system to produce first encrypted segments;

a second encrypter that encrypts the identified segments of content using a second encryption method associated with a second conditional access system to produce second encrypted segments;

wherein the programmed processor further receives the first and second encrypted segments and replacing the identified segments of content with the first encrypted content and the second encrypted content in the digital content, to produce the multiple selectively encrypted VOD content;

means for storing the multiple selective encrypted VOD content;

means for receiving an order for the VOD content specifying delivery to a target decoder;

means for determining what CA encryption system is associated with the order; and

wherein the programmed processor strips all encrypted segments from the multiple selectively encrypted content that are not associated with the order to produce single selectively encrypted VOD content.

10. The encoder according to claim 9, wherein the programmed processor further associates a program identifier with the single selectively encrypted VOD content, wherein the same PIDs are used for encrypted and unencrypted segments of content, and sends the single selectively encrypted VOD content to the target decoder.

11. A selectively encrypted video on demand (VOD) system, comprising:

a VOD server storing multiple selective encrypted VOD content;

program means running on a programmed processor for receiving an order for the VOD content specifying delivery to a target decoder, and for determining a CA encryption system associated with the order;

wherein, in response to the order, the VOD server strips all encrypted segments from the multiple selectively encrypted content that are not associated with the order to produce single selectively encrypted VOD content;

a target decoder addressable by the VOD server; and

means for sending the single selectively encrypted VOD content from the VOD server to the target decoder.

12. The system according to claim 11, wherein:

the VOD server carries out a programmed process that examines unencrypted data representing digital content to identify segments of content for encryption;

and further comprising:

a first encrypter that encrypts the identified segments of content using a first encryption method associated with a first conditional access system to produce first encrypted segments;

a second encrytper that encrypts the identified segments of content using a second encryption method associated with a second conditional access system to produce second encrypted segments; and

wherein the VOD server replaces the identified segments of content with the first encrypted content and the second encrypted content in the digital content, to produce the multiple selectively encrypted VOD content.

13. The system according to claim 12, wherein the VOD server further associates a program identifier with the single selectively encrypted VOD content, wherein the same PIDs are used for encrypted and unencrypted segments of content.

14. The system according to claim 11, wherein the decoder comprises a television Set-top box.

15. The system according to claim 11, wherein the VOD server resides at a cable hub.

16. The system according to claim 11, wherein the VOD server resides at a cable system head end.

17. An electronic storage medium storing selectively encrypted video on demand (VOD) programming, comprising:

a file representing multiple selective encrypted VOD content comprising:

segments of unencrypted VOD content;

first encrypted segments of VOD content encrypted using a first encryption method associated with a first conditional access system;

second encrypted segments of VOD content encrypted using a second encryption method associated with a second conditional access system;

the first and second encrypted segments of VOD content representing the same segment of VOD content when not encrypted;

a first segment of code that when executed operates to remove one of the first and second encrypted segments of VOD content from the multiple selective encrypted VOD content to produce single selectively encrypted content for transmission to a target decoder.

18. The electronic storage medium according to claim 17, wherein the first segment of code operates to remove one of the first and second encrypted segments of VOD content upon receipt of an order for the VOD content specifying delivery to a target decoder, and upon determining which CA encryption system is associated with the order.

19. The electronic storage medium according to claim 17, further comprising a second segment of code that sends the single selectively encrypted VOD content to the target decoder.

20. The electronic storage medium according to claim 17, further comprising a third segment of code that associates a program identifier with the single selectively encrypted VOD content, wherein the same PIDs are used for encrypted and unencrypted segments of content.

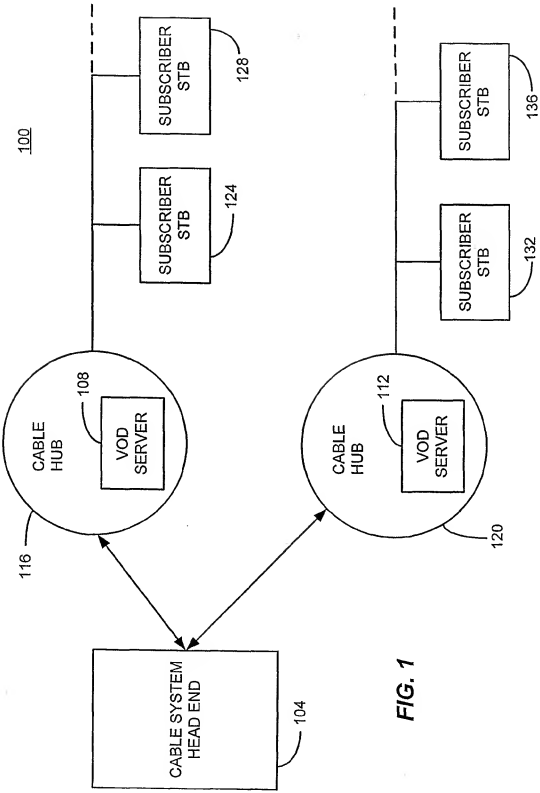

100
CABLE SYSTEM HEAD END
104
CABLE HUB
VOD SERVER
108
116
CABLE HUB
VOD SERVER
112
120
SUBSCRIBER STB
124
SUBSCRIBER STB
128
SUBSCRIBER STB
132
SUBSCRIBER STB
136

FIG. 1

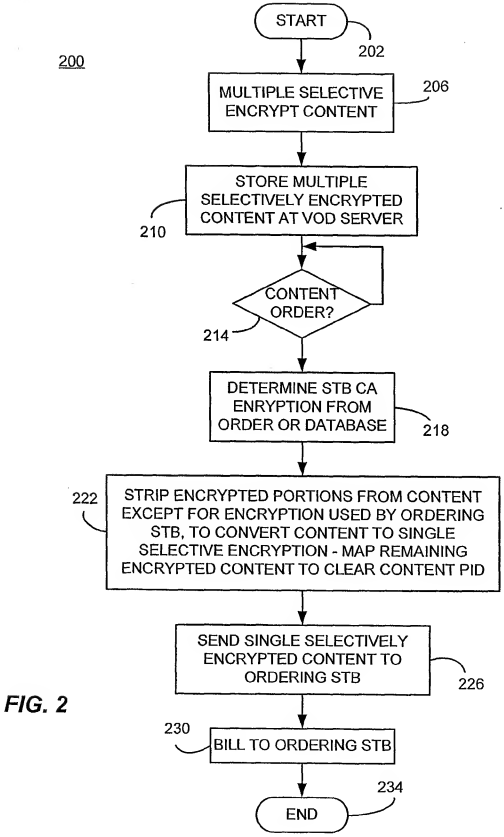

200
START
202
MULTIPLE SELECTIVE ENCRYPT CONTENT
206
STORE MULTIPLE SELECTIVELY ENCRYPTED CONTENT AT VOD SERVER
210
CONTENT ORDER?
214
DETERMINE STB CA ENRYPTION FROM ORDER OR DATABASE
218
222
STRIP ENCRYPTED PORTIONS FROM CONTENT EXCEPT FOR ENCRYPTION USED BY ORDERING STB, TO CONVERT CONTENT TO SINGLE SELECTIVE ENCRYPTION - MAP REMAINING ENCRYPTED CONTENT TO CLEAR CONTENT PID
SEND SINGLE SELECTIVELY ENCRYPTED CONTENT TO ORDERING STB
226
230
BILL TO ORDERING STB
234
END

FIG. 2

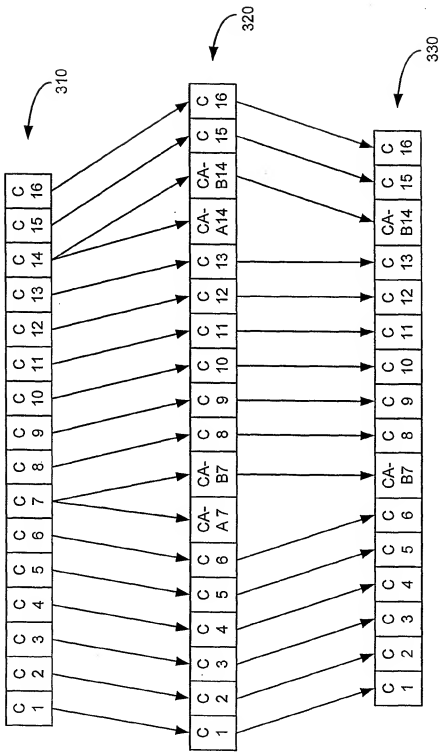

310
320
330
C 1
C 2
C 3
C 4
C 5
C 6
C 7
C 8
C 9
C 10
C 11
C 12
C 13
C 14
C 15
C 16
CA-A7
CA-B7
CA-A14
CA-B14

FIG. 3

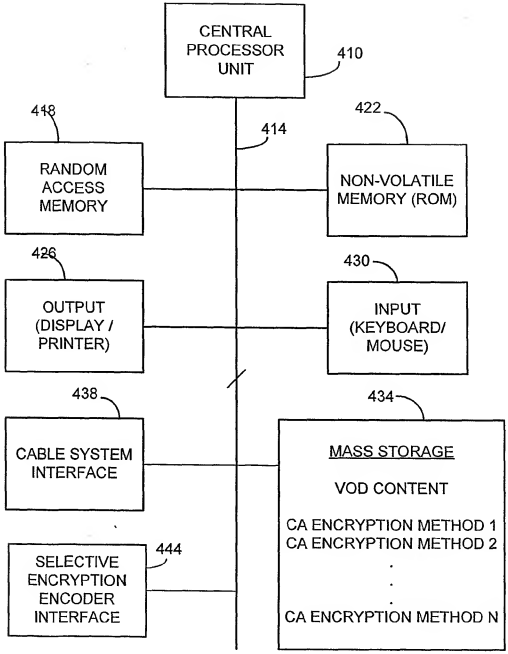

CENTRAL PROCESSOR UNIT
410
418
414
422
RANDOM ACCESS MEMORY
NON-VOLATILE MEMORY (ROM)
426
430
OUTPUT (DISPLAY / PRINTER)
INPUT (KEYBOARD/ MOUSE)
438
434
CABLE SYSTEM INTERFACE
MASS STORAGE
VOD CONTENT
CA ENCRYPTION METHOD 1
CA ENCRYPTION METHOD 2
.
.
.
CA ENCRYPTION METHOD N
444
SELECTIVE ENCRYPTION ENCODER INTERFACE
400

FIG. 4